Exhibit 2

Computer Forensics Investigation Report – *Benthos v. Etra*

Case Number: 22-cv-3384 (S.D.N.Y.)
Case Name: *Benthos v. Etra*
Defendant's Name: Aaron Etra
Date of Report: [Date]

Devices and Accounts Analyzed

List the devices and accounts examined during the investigation, including (but not limited to):

1. Apple computer
2. Apple iPhone
3. Cloud storage accounts
4. Additional electronic devices, removable storage media, or digital accounts

Methodology

The following forensics analysis techniques will be employed during the investigation:

1. Precautionary Measures: a. Utilize a hardware write block device or other industry-standard techniques to protect the integrity of the data on the Devices and Media.
2. Forensic Imaging:
    a) Create full forensic images of each Device and Media/account (the "Etra Images"), including allocated, unallocated, and host-protected areas (to the extent possible).
    b) Maintain a log to record the following information, where applicable:
        i. Date and time of Device or Media provision and imaging.
        ii. Time set in the BIOS or system clock during imaging.
        iii. Boot order recorded in the BIOS of the Device or Media during imaging.
        iv. Make, model, and serial number of the Device.
        v. Username associated with any Media.
        vi. Identifying marks or labels on any Device or Media. vii. Tool and/or method used to create forensic images. viii.MD5 and SHA-1 hash values of the data collected from the Device or Media.

3. Forensic Analysis:

    a) Analyze the Etra Images to identify any evidence relating to the integrity, authenticity, and completeness of the data.

    b) Conduct a forensic examination to review activity involving the creation, downloading, transfer, deletion, obfuscation, or destruction of files from August 12, 2020, onward.

    c) Attempt to recover and examine files transferred, deleted, obfuscated, or destroyed since August 12, 2020, following the procedures set forth herein.

4. Reporting:

    a) Develop a "Report" that contains the following information related to the files and names of relevant individuals found on the Etra Images, including any files stored and associated names of relevant individuals in the Cloud (Apple iCloud, Dropbox, etc.):

        i. A comprehensive list of all relevant files, including file names, file types, file sizes, and creation, modification, and last accessed dates.

        ii. A brief description or summary of the content of each file, where applicable.

        iii. Names of relevant individuals associated with each file, including but not limited to authors, recipients, or individuals mentioned within the file.

        iv. Any email addresses, phone numbers, or other contact information associated with the relevant individuals.

        v. Any relevant metadata associated with each file, such as geolocation data, device information, or software used to create or modify the file.

        vi. The location (e.g., folder path) of each file on the Device or Media, as well as any Cloud storage platforms.

        vii. Any evidence of file transfer, deletion, obfuscation, or destruction, including dates, methods, and tools used.

        viii. Information about any file recovery efforts, including the success or failure of such efforts and any limitations encountered.

        ix. Any relevant screenshots, images, or visual representations that can provide additional context or evidence for the analyzed files.

    b) Address, to the extent technically feasible and ascertainable, the activities and events involving deletion, obfuscation, destruction, damage, or transfer of files or other material from August 2020 onward.

Findings

Present the results of the investigation for each of the categories mentioned in the objectives. Organize this section by sub-category.